

(19)日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11)特許出願公表番号

特表2002-512409

(P2002-512409A)

(43)公表日 平成14年4月23日 (2002.4.23)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テ-マコ-ト <sup>8</sup> (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 F 5 B 0 8 5
H 0 4 Q 7/38		H 0 4 M 1/66	5 K 0 2 7
H 0 4 M 1/66		H 0 4 B 7/26	1 0 9 M 5 K 0 6 7
			1 0 9 R

審査請求 未請求 予備審査請求 有 (全 19 頁)

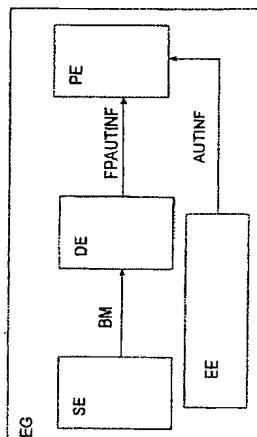
(21)出願番号	特願2000-545128(P2000-545128)
(86) (22)出願日	平成10年8月21日(1998.8.21)
(85)翻訳文提出日	平成12年10月20日(2000.10.20)
(86)国際出願番号	P C T / D E 9 8 / 0 2 4 5 7
(87)国際公開番号	W O 9 9 / 5 4 8 5 1
(87)国際公開日	平成11年10月28日(1999.10.28)
(31)優先権主張番号	1 9 8 1 7 7 7 0 . 4
(32)優先日	平成10年4月21日(1998.4.21)
(33)優先権主張国	ドイツ (DE)
(81)指定国	E P (A T, B E, C H, C Y, D E, D K, E S, F I, F R, G B, G R, I E, I T, L U, M C, N L, P T, S E), B R, C A, C N, J P, K R, U S

(71)出願人	シーメンス アクチエンゲゼルシャフト S I E M E N S A K T I E N G E S E L L S C H A F T ドイツ連邦共和国 D-80333 ミュンヘン ヴィッテルスバッハーブラツツ 2
(72)発明者	クラウス-ベーター カールマン ドイツ連邦共和国 ミュンヘン シュトラーベルガー シュトラーセ 8
(74)代理人	弁理士 矢野 敏雄 (外4名) Fターム(参考) 5B085 AE02 AE25 AE26 5K027 AA11 BB09 EE11 HH11 HH23 HH24 5K067 AA21 BB04 EE02 HH32 HH36

(54)【発明の名称】 電子機器、およびこの機器のユーザの認証を行う方法

(57)【要約】

機器は生理学的特徴 B M (例えば指紋) を検出するセンサと、認証データ A U T I N F (例えばP I N) を入力する入力装置とを有している。この機器のデータ処理装置 D E は生理学的特徴 B M から認証情報 F P A U T I N F を求める。この情報は、入力装置 E E を介して入力される認証情報 A U T I N F と同じ検査装置 P E で検査される。これによりこの機器 E G を種々のユーザは生理学的特徴のためのセンサのない装置と同様に利用できる。認証プロトコル (例えば移動電話ではS I Mカード) を変更する必要はなく、これにより生理学的特徴による認証が可能となる。



**【特許請求の範囲】**

【請求項1】 電子機器、例えば情報処理または通信用の機器において、

- a) 機器のユーザの生理学的特徴 (B M) 、例えば指紋を検出するセンサ装置 (S E) と、
- b) ユーザの認証に利用される情報 (F P A U T I N F) を検出された生理学的特徴から求めるデータ処理装置 (D E) と、
- c) 情報を入力する入力装置 (E E) 、および該入力装置を介して認証に利用される情報 (A U T I N F) を入力する手段と、
- d) 求められたかまたは入力された認証情報を検査し、かつ検査が有効であった場合に当該のユーザに対して機器の機能を解放する検査装置 (P E) とを有することを特徴とする電子機器。

【請求項2】 前記データ処理装置 (D E) は、有効な認証の検査のために入力装置を介して入力される認証情報 (P I N) が権限を有するユーザの生理学的特徴から求められた認証情報 (F P P I N) と同一であるように構成されている、請求項1記載の機器。

【請求項3】 前記データ処理装置 (D E) は検出されたユーザの生理学的特徴から当該のユーザの認証に利用される情報 (F P A U T I N F 1, . . . , F P A U T I N F n) を求める複数のプロセス (M 1, . . . , M n) を使用できる、請求項1または2記載の機器。

【請求項4】 前記データ処理装置は権限を有するユーザに対して、生理学的特徴から認証情報を求める複数のプロセスのうち所望のプロセスを選択させる、請求項3記載の機器。

【請求項5】 ユーザの生理学的特徴から求められた認証情報 (F P A U T I N F) を表示する手段を有する、請求項1から4までのいずれか1項記載の機器。

【請求項6】 ユーザはユーザに固有の生理学的特徴を用いてまたは認証情報を情報入力装置を介して入力することにより認証を行う手段を有しており、第1のケースではユーザの生理学的特徴をセンサ装置により検出し、検出された生

理学的特徴から認証に利用される情報を求めて検査装置により検査し、第2のケースではユーザが入力装置を介して入力した認証情報を同じ検査装置で検査することを特徴とする機器ユーザの認証を行う方法。

【請求項7】 a) センサ装置の測定データから特徴ベクトルを求めるステップと、  
b) 求められた特徴ベクトルからベクトルを量子化するステップと、  
c) ベクトルの量子化の結果に対応する認証情報を検査するステップとを有する  
請求項6記載の機器ユーザの認証を行う方法。

**【発明の詳細な説明】****【0001】**

利用する前にユーザが認証ないしオーセンティフィケーションを行わなくてはならないきわめて様々の電子機器が知られている。その主たる例は種々の構成のコンピュータ（情報処理機器）や通信機器、例えば移動電話などである。これらの機器には一般に不正使用に対して例えばパスワードにより保護されているものがある。他の機器は単に所定の機能のみを不正アクセスに対して（例えばいわゆる個人識別番号PINによって）保護している。これには所定のデータまたはサービスへのアクセスの保護も属している。これが機器により使用されるのではなくてコンピュータネットワークまたは通信ネットワークにより使用される場合でもそうである。

**【0002】**

今日頻繁に使用される形式の認証情報の入力は機器のキーボードを介した入力である。入力後に入力された情報の正当性、ひいては入力を行ったユーザの権限が機器またはコンピュータネットワークまたは通信ネットワークの検査装置で検査される。GSM規格に準拠した移動電話では、これは機器のいわゆるSIMカード上のデータ処理装置を用いて、入力されたPINがSIMカードに記憶された情報に適合するか否かを検査することにより行われる。適合する場合にはSIMカードにより移動電話が使用可能となる。GSM規格に準拠してPINが機器内に記憶されず、ロックされた状態でSIMカードに記憶されている場合、電話の顧客のセキュリティは上昇する。

**【0003】**

しばらく前からユーザの認証を他の形式で行うことのできる技術が使用されている。この技術はユーザに固有の生理学的特徴を特別のセンサによって検出することに基づいている。この主な例は指紋検出センサである。別の生理学的特徴は例えば人間の目の網膜組織または人間の声の特性であり、これらも同様に数種の機器で使用されている。

**【0004】**

通常はセンサによって検出された特徴は機器または通信ネットワークのデータ

処理装置で権限を有するユーザの既知の特徴と比較され、充分に一致する場合に所望のサービス、必要なデータまたは選択された機器の機能へのアクセスが解放される。

#### 【0005】

幾つかのタイプの機器では、前述の2つの形式の認証が相互に組み合わせると有意義である。例えば移動電話では、ユーザが指紋センサによって電話を利用できるだけでなく、PINを他の人物とシェアしたり、固有のSIMカードで機器を与えられている権限の範囲内で利用できるように利用できたりするほうが望ましい。さらに指紋を介した認証は偶発的にエラーを発生したり、または実行不能になったりする。これは例えばユーザの手が汚れていたり、ユーザが手袋を着けていたりする場合である。これらの理由またはその他の理由から望ましいのは（または必要なのは）、機器の1人または複数人のユーザが異なる手法で認証を行えることである。生理学的な認証はこのケースではPIN入力による認証と並んで行われる。GSM規格に準拠する移動電話では、この規格がPIN入力による認証手段を強制的に予め定めている。

#### 【0006】

前述の状況から、従来の生理学的な認証プロセスはGSM規格に準拠する移動電話では不可能であることがわかる。なぜならGSM規格に対する互換性の理由から、SIMカードを用いたPINによる認証が必ず要求されるからである。さしあたり可能に見える手段として、PINを機器内に記憶し、検出された指紋と権限を有するユーザの記憶された指紋と一致して検査が有効である場合に記憶されているPINをSIMカードへ譲渡して検査することが考えられるが、これは排除される。なぜならPINを移動電話においてSIMカード内部以外の別の場所に記憶することはセキュリティ上の理由からGSM規格により禁じられているからである。生理学的な認証はこの場合には付加的なセキュリティ手段として考慮される。ただしこのような付加的なセキュリティ手段はPIN入力による認証の高い安全性からすれば不必要であり、多くのユーザが受け入れがたく感じるはずである。

#### 【0007】

本発明の基礎とする課題は、生理学的なユーザの認証とPIN入力による認証との組み合わせをGSM規格または類似のケースの移動電話においても可能にし、それぞれの形式の認証を充分に活用できるようにする技術的思想を提供することである。ユーザはどちらの形式の認証を使用したいかという選択権を有している。ただし特に選択されたユーザ（例えば機器の所有者）が機器での2つの認証形式の論理AND結合を調整できる手段を有するようにすることもできる。この課題は特許請求の範囲に記載の機器または方法により解決される。

#### 【0008】

本発明では、ユーザの生理学的特徴がセンサ装置により検出され、検出された生理学的特徴から認証に利用される情報が数学的プロセスを用いて求められる。これにより生理学的特徴を評価する最終段階で認証情報が生じ、この情報はユーザが情報入力装置（例えばキーボード）を介して入力した認証情報を検査するのと同じ検査装置で検査される。最も簡単なケースでは指紋の評価の結果はユーザがキーボードを介して入力したPINと同じものとなる。ただしこのPINは機器に記憶されるのではなく、センサ装置によって検出されたユーザの生理学的特徴から計算される。

#### 【0009】

センサ装置によって検出された生理学的特徴を評価する形式により、この形式の認証はキーボードの入力を介した認証の結果と同等となり、認証の妥当性を検査する通常のインターフェースを変更しなくともよくなる。特に規格化された何らかのプロトコルを変更する必要はない。認証の2つの手法は問題なく並列的に使用することができる。ユーザはいつでもどんな状態でも2つの手法を自由に選択できる。もちろんAND結合を使用して2つの認証手法が有効に経過したユーザのみに許可を与えるように構成することもできる。

#### 【0010】

以下に本発明を有利な実施例に則して図を用いて詳細に説明する。

#### 【0011】

図1には、全ての方法および装置が機器内に集積されている本発明の実施例が示されている。

**【0012】**

図2には検査装置が機器内に存在している本発明の実施例が示されている。

**【0013】**

図3には認証情報を表示する表示装置が機器に集積されている本発明の実施例が示されている。

**【0014】**

本発明に典型的でしかも重要な実施例はGSM規格に準拠する移動電話であり、これはユーザの認証に指紋センサを使用する。この指紋センサは図1に示されたセンサ装置SEの特殊な例である。機器EGのユーザが指をこの指紋センサに載せて、機器が例えばPINまたはSuperPINまたはPIN2（部分的にメーカーに依存する）などの入力の認証を行うのを待機していると、指紋センサが当該のユーザの相応の生理学的特徴BMを検出し、これをデータ処理装置DEへ送出する。

**【0015】**

GSM移動電話の場合、このデータ処理装置は移動電話に既に設けられているプロセッサと、このプロセッサ上で動作するソフトウェアとである。しかし他方では指紋センサは（または一般にセンサ装置は）固有のプロセッサユニットを介して使用され、このプロセッサユニット上で指紋認識を管理する特別のソフトウェアが動作する。これによりデータ処理装置は本発明の範囲では完全にまたは部分的にセンサ装置内に組み込まれている。指紋認識自体は生理学的特徴を認識する他の手法と同様に、データ処理装置の実現形態すなわち種々のコンフィグレーション（およびサブシステムでのパーティショニングまたは周知のハードウェアモジュールの統合）が当業技術者には充分に周知であるので、この部分に関しては本発明のセキュリティの実現に特に問題はない。

**【0016】**

本発明によれば、データ処理装置は検出された生理学的特徴からユーザの認証に適した情報を求める。最も簡単なケースではこれは権限を有すると見なされるユーザのSIMカード上にロックされた状態で記憶されたPIN（ないしPIN2その他）である。このPINはユーザが移動電話のキーボード（情報入力装置

) を介して入力したのと同様に SIMカードへ引き渡され、検査される。次に当業技術者には周知の GSM 規格に定められている検査過程が移動電話の検査装置 (SIMカード、場合により機器のデータ処理装置と関連している装置) 内で動作する。認証情報 F P A U T I N F が正しい場合、すなわち SIMカード上に記憶された PIN と一致する場合には、認証により保護されている機器の機能 (例えばネットワークアクセスなど) が解放される。

#### 【0017】

前述の本発明の手段の重要な利点は、ユーザが権限を有している場合に指紋認識部がユーザの PIN を SIMカードへ引き渡すことである。というのはこれにより GSM 規格のセキュリティプロトコルを全く変更しなくて済むからである。他の基礎的と思われる手段にはこの有利な特性が存在しない。いずれにしろ他の手段ではキーボードを介した付加的な PIN の入力が必要となるか、または GSM 規格の回避ないし変更が必要となる。キーボードを介した付加的な PIN の入力は、指紋認識を PIN 入力に加えた付加的なセキュリティ手段として考慮する場合にのみ有効である。

#### 【0018】

このような付加的な認証はもちろん本発明によっても可能である。この場合センサデータから求められた認証情報は SIMカードへ伝送しなくてもよい。その代わりに例えば故意に誤った PIN を SIMカードへ伝送してしまったり、または入力エラーまたは入力の中止その他などがシミュレートされたりすることがある。これに対して SIMカードは新たに PIN 入力を要求する。入力された PIN が求められた PIN と一致するかまたは互換的である場合には、データ処理装置 DE はこの PIN を SIMカードへ伝送し、これに応じて解放が許可される。

#### 【0019】

もちろんセンサデータから求められた PIN は必ずしも SIMカードの PIN と同一でない場合もありうる。前述の規格または他の機器ではそのつど適切なセキュリティプロトコルが許可する場合には、検査装置が 2 つの異なる認証情報によって、これらが相互に適合するか否かを検査することができる。

#### 【0020】

GSM規格に準拠しない他の機器では、センサデータから計算された認証情報 F P A U T I N F がセンサデータによるただ1つの認証（すなわち P I N 入力と同時の認証またはこれと独立の認証）で有る場合、キーボードを介して入力された認証情報 A U T I N F と異なっていることがあるが、2つの情報が権限を有するユーザを指示すれば、検査装置はこれらが同時に適合していると認識する。

#### 【0021】

生理学的特徴 B M から得られた認証情報 F P A U T I N F に対する計算プロセスとして基本的に全ての数学的なシミュレーション（関数）が考慮され、指紋または他の生理学的特徴 B M に他の形式の（一般には英数字によって符号化された）認証情報 A U T I N F が割り当てられる。ここで次の条件を満足しなければならない。すなわち

- a) 充分に類似の生理学的特徴 B M から同じ認証情報 F P A U T I N F が導出され、
- b) 充分に異なる生理学的特徴 B M から異なる認証情報 F P A U T I N F が導出され、
- c) 不正のユーザにとっては、認証情報 F P A U T I N F を生理学的特徴 B M またはこの特徴 B M の知識から求める（例えば推測する）ことが実質的に不可能である、

ことである。

#### 【0022】

条件 a) は指紋認識が小さなノイズに対しても充分にローバストで有ることを保証する。そうでないと権限を有するユーザが拒絶される割合がきわめて高くなってしまうからである。条件 b) はこれに対して、異なるユーザの指紋が充分に高い確率で種々の認証情報 F P A U T I N F を導出するように設けられている。

条件 c) の意義は明らかである。

#### 【0023】

当業者には（場合によって適切さの多少はあるが）この要求を満足する種々の数学的シミュレーションが周知である。これらの特性を有するシミュレーションはいわゆるベクトル量子化によって与えられる。当業者に周知の手法については

ここでは本発明の理解に必要であると思われる個所以外は説明しない。

#### 【0024】

この手法を本発明の目的に使用する際にはまず、センサ装置によって検出された生理学的特徴がいわゆる特徴ベクトルの形式へ移されることを前提とする。この仮定は実際には何らの限定にもならない。なぜならセンサデータはつねに  $n$  個の測定データ（特徴ベクトル）の順序づけられた  $n$  個のグループとして表されるからである。特徴ベクトルは  $n$  次元の空間を形成する。この空間内にはパターンベクトルの集合（コードブックベクトル）が存在し、距離尺度（生理学的特徴に対する類似の度合）が規定される。各パターンベクトルに対して空間内のセルが存在し、このセルはセル内の各特徴ベクトルに相応し、パターンベクトルは当該の距離尺度の範囲内で次に存在するパターンベクトルのセルであることにより規定されている。

#### 【0025】

各パターンベクトルには認証に基本的に適した情報が割り当てられている。1つのパターンベクトルには正確な認証情報（例えば真のPIN）が割り当てられている。前述の説明から明らかなように、検出されたセンサデータに相応する所定の特徴ベクトルに対して次に存在するパターンベクトルを求めるとき、当該のユーザが権限を有する場合には正確な情報（真のPIN）が導出され、そうでない場合には誤った認証情報が送出される。このプロセスのエラーレートは権限を有するユーザの生理学的特徴に関連する特徴ベクトルがパターンベクトルの1つであることが保証される場合に最適化することができる。これはこのシステムを初期化フェーズで権限を有するユーザの生理学的特徴に適応させること（コードブック適応化）により達成される。

#### 【0026】

ベクトル量子化は本発明に関連して使用できる唯一の手法ではない。当業者にはここで説明しない他の手法も実施可能である。

#### 【0027】

認証情報 FPAUTINF をユーザの生理学的特徴からベクトル量子化により計算することは（本明細書に基づくならば）本来機器での“PINの記憶”に結

びついている。なぜならコードブックの各パターンベクトルには基本的に可能な認証情報 F P A U T I N F が割り当てられているからである。ただしこれはほぼ全てのケースで（1人のユーザ、すなわち権限を有するユーザの特徴ベクトルを除いて）実際には認証には適さない。つまり例えば5桁の英数字の P I N では理想的には全ての可能な P I N が記憶されてこれらのそれぞれに1つずつパターンベクトルが割り当てられるのであるが、パターンベクトルが充分に正確に検出された場合にしかセンサ内で妥当な P I N にアドレシングできない。したがって正確な P I N は“機器内に記憶されている”にもかかわらず、可能な P I N の数が大きくなりすぎ、正確な生理学的特徴を有するユーザ以外は見いだせなくなってしまうのである。こうした状況は規格によって P I N を機器に記憶することが禁止されている場合には考慮されていない。

#### 【0028】

G S M 規格では P I N を機器に記憶することは許可されていない。ただし P I N を変更する必要は頻繁に生じる。これは例えば P I N が第3者に知られてしまった場合などである。ただし本発明では P I N を指紋から求める（すなわち計算する）ので、指紋または他の生理学的特徴の交換が可能でないかぎりこれはまず不可能である。それでもユーザに P I N を変更する手段を与えるのであれば、本発明の有利な実施形態により、ただ1つの計算プロセスに代えて機器内のこの種のプロセスの全ての集合を同等に使用できるように構成する。個々の計算プロセスには連続番号が割り当てられており、これに対して権限を有するユーザは使用するプロセスをいつでも変更できる。同一の指紋 B M に対する各プロセス M 1, . . . , M n は他の P I N (F P A U T I N F 1, . . . , F P A U T I N F n ) を計算するので、ユーザは多数の P I N をどのプロセスで計算させるかを選択する。

#### 【0029】

本発明の実施例は同様にベクトル量子化によっても実現できる。ここでコードブックだけでなく、パターンベクトルの複数のコードブックも設けられている。各コードブックは所定の番号を有しており、この番号を介して選択可能である。他のプロセスはおそらくパラメータに依存している。本発明ではこのパラメータ

を変更することにより、他の数学的なシミュレーションも形成する。パラメータの依存性が充分に複雑であれば、実際にはパラメータを変更しても認証情報の変更は推測が不可能になる。所定のタイプのニューラルネットワーク（いわゆるマルチレイヤペーセptron）はこの種のシミュレーションを実現するのに適する。このニューラルネットワークに基づく手段ではPINは実際にはどこにも記号シーケンスとしては記憶されておらず、単に（暗示的にロックされた状態）ネットワークアーキテクチャに重みづけ係数として記憶される。

#### 【0030】

本発明のこの実施例では、特に多数の人物の異なるパスワードのシーケンスが完全に異なる目的または機器に対して必要となる観点から考慮される。多数のパスワードに留意することはますます困難となるはずである。複数のプロセスM1, ..., Mn（数学的シミュレーション）を複数の認証情報（FPAUTIN F1, FPAUTINF2）の唯一の特徴ベクトル（センサデータの集合）からの計算に使用する場合、ユーザに固有の公けにできない生理学的特徴を検出する際の問題が適切なセンサにより低減される。

#### 【0031】

所定のプロセスを選択するためには、単にユーザの操作表面に設けられたコンテクストでこの種のプロセスのインデクスを入力すればよい。これによりソフトウェアごとにデータ処理装置が相応に構成できる。

#### 【0032】

もちろん複数の人物の生理学的特徴を1つまたは複数の正しいPINと結合することもできる。機器が例外として1人の人物としか結合されていない場合、すなわち正確に1つのSIMカードしか使用されない場合には、解放は付加的に他のセキュリティ機構、例えば機器のコードなどに結合できる。本発明によればここではそれぞれの形式の柔軟性と高い安全性、規格に対する互換性が得られる。

#### 【0033】

PINを変更する場合、本発明の特に有利な別の実施例では、認証情報の表示用のディスプレイが設けられている。この種のディスプレイはこの種の多数の機器ですでに始めから存在しているので、これをこの目的のために利用できる。ユ

ユーザがキーボードを介して入力した認証情報 A U T I N F (例えば P I N) を S I M カードに適合する情報に変更しようとすると、幾つかの計算プロセスでは場合により可能な全ての記号の数字の組み合わせが P I N として使用できない。なぜなら例えばコードブックが可能な全ての P I N の数よりも小さいからである。このケースでは使用される計算プロセスのパラメータの変更 (例えばコードブック番号の変更、またはニューラルネットワークのパラメータの変更) を行えば、P I N をパターンベクトルに割り当てて個人のパターンベクトルに対応する P I N を変更するには充分である。その後は S I M カード上の P I N (または一般に入力すべき P I N) を知らなければこの意味では変更できなくなる。しかもこれは本発明の課題に対する更なる利用のために必要である。変更された P I N は権限を有するユーザには有利には相応に P I N を変更後に機器のディスプレイに 1 回だけ短時間表示させることにより知らせることができる。他の手段 (例えば新たな P I N を後から提示すること) も可能である。

#### 【0034】

本発明はもちろん移動電話、例えば G S M 規格に準拠する移動電話に限定されるものではない。当業者には前述の説明に基づいて、本発明を他の機器または他のシステムにおいて実現することも困難ではない。

#### 【0035】

特に本発明は検査ユニット P E が機器内に集積されているケースのみに限定されない。図 2 には機器の重要な例が示されており、ここでは機器は例えば通信ネットワークを介して少なくとも 1 つの他の機器と接続され、検査装置もネットワーク内に存在している。またデータ処理装置またはデータ処理ユニット D E の一部、すなわちユーザの生理学的特徴 B M から認証情報 F P A U T I N F を計算することを管理する部分も必ずしも機器内に存在していなくてもよい。もちろん機器は集積されたセンサ装置 S E または集積されたキーボード E E を有していなくてもよい。装置を外部モジュールのかたちで機器に接続してもよいことも明らかである。本発明の実施例は方法の請求項により保護されるべきである。

#### 【図面の簡単な説明】

#### 【図 1】

全ての方法および装置が機器内に集積されている本発明の実施例を示す図である。

【図2】

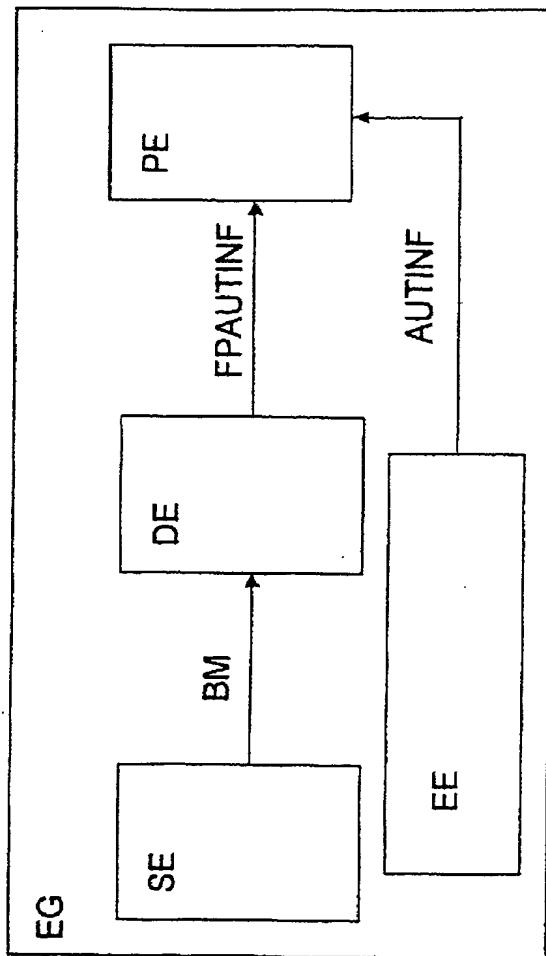
全ての方法および装置が機器内に集積されている本発明の実施例を示す図である。

【図3】

認証情報を表示する表示装置が機器に集積されている本発明の実施例を示す図である。

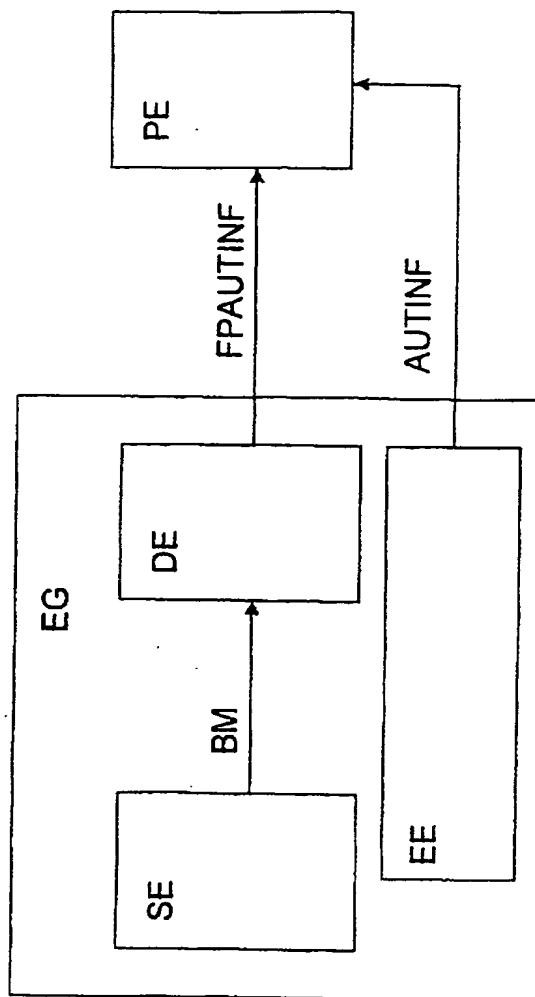
【図1】

FIG 1



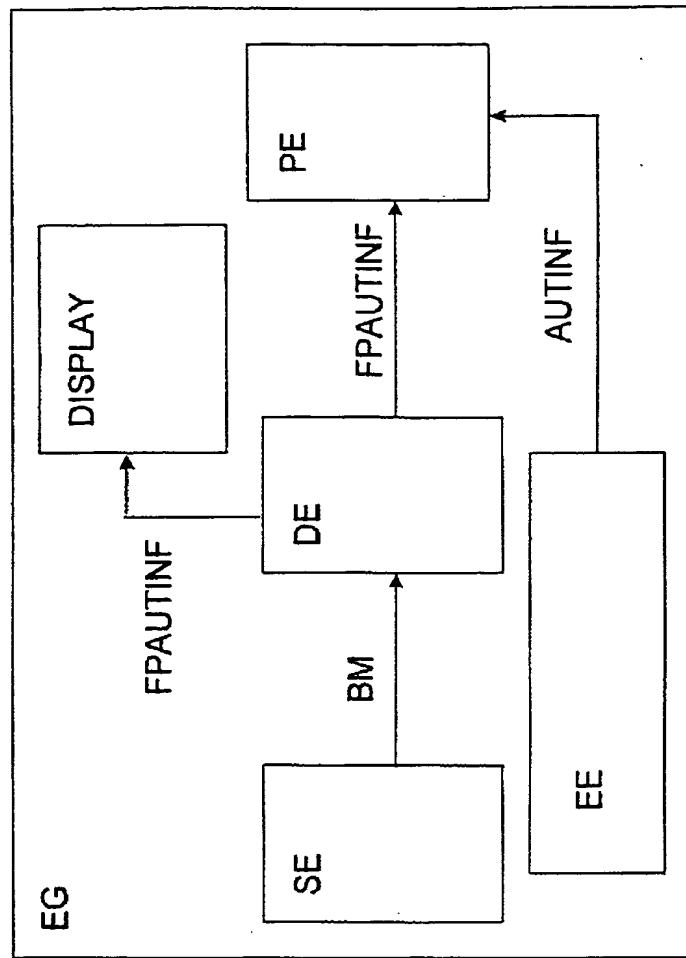
【図2】

FIG 2



【図3】

FIG 3



## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

Int. Application No.  
PCT/DE 98/02457

A. CLASSIFICATION OF SUBJECT MATTER		
IPC 6 G07C9/00 H04Q7/38 G07F7/10		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) IPC 6 G07C G07F H04Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 11750 A (SUBBIAH SUBRAMANIAN ;LI YANG (US); RAO D RAMESK K (US)) 19 March 1998 see page 3, line 8 - page 4, line 29 see page 5, line 34 - page 8, line 24; figures	1,3
Y	DE 25 33 699 A (SIEMENS AG) 10 February 1977 see page 3, line 1 - line 12 see page 5, line 1 - line 7; figures; examples	2,6
Y	---	2,6
	---	-/-
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.		<input checked="" type="checkbox"/> Patent family members are listed in annex.
* Special categories of cited documents :		
'A' document defining the general state of the art which is not considered to be of particular relevance		
'E' earlier document but published on or after the international filing date		
'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)		
'O' document referring to an oral disclosure, use, exhibition or other means		
'P' document published prior to the international filing date but later than the priority date claimed		
'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention		
'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone		
'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art		
'S' document member of the same patent family		
Date of the actual completion of the international search	Date of mailing of the international search report	
27 January 1999	03/02/1999	
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 661 0901 Fax: (+31-70) 340-3016	Authorized officer Meyl, D	

## INTERNATIONAL SEARCH REPORT

Int. Search Application No.  
PCT/DE 98/02457

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 731 426 A (JOHNSON NELDON P) 11 September 1996 see abstract; figures see column 5, line 7 - line 39 see column 6, line 36 - column 7, line 31	1,2,6
A	EP 0 504 616 A (ASCOM AUTELCA AG) 23 September 1992 see abstract; claims; figures	1-3,6
A	WO 96 08093 A (MYTEC TECHNOLOGIES INC) 14 March 1996 see abstract; figures see page 3, line 2 - line 18	1,2,6
A	WO 97 04375 A (SIEMENS AG OESTERREICH ;FORER JOSEF (AT); KAUF OTTO (AT)) 6 February 1997	
A	DE 93 04 488 U (SIEMENS AG) 29 July 1993	

## INTERNATIONAL SEARCH REPORT

Information on patent family members

Int'l Application No  
PCT/DE 98/02457

Patent document cited in search report	Publication date	Patent family member(s)			Publication date
WO 9811750	A 19-03-1998	AU	4341797	A	02-04-1998
DE 2533699	A 10-02-1977	NONE			
EP 0731426	A 11-09-1996	US	5598474	A	28-01-1997
		AU	693655	B	02-07-1998
		AU	4805096	A	19-09-1996
		BR	9600961	A	30-12-1997
		CN	1137659	A	11-12-1996
		JP	9114986	A	02-05-1997
EP 0504616	A 23-09-1992	NONE			
WO 9608093	A 14-03-1996	US	5541994	A	30-07-1996
		US	5680460	A	21-10-1997
		AU	689946	B	09-04-1998
		AU	3339095	A	27-03-1996
		BR	9509002	A	02-06-1998
		CA	2199034	A	14-03-1996
		CN	1157677	A	20-08-1997
		EP	0780040	A	25-06-1997
		JP	10505474	T	26-05-1997
		US	5737420	A	07-04-1998
		US	5832091	A	03-11-1998
WO 9704375	A 06-02-1997	EP	0782724	A	09-07-1997
DE 9304488	U 29-07-1993	NONE			

**Warning: PAJ Data was not available on download time. You may get bibliographic data in English later.**

**\* NOTICES \***

**JPO and INPIT are not responsible for any damages caused by the use of this translation.**

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. \*\*\*\* shows the word which can not be translated.
3. In the drawings, any words are not translated.

---

## **CLAIMS**

---

**[Claim(s)]**

**[Claim 1]**Apparatus for electronic equipment characterized by comprising the following, for example, information processing, or communication.

- a) A sensor apparatus (SE) which detects physiological characterization of a user of apparatus (BM), for example, a fingerprint.
- b) A data processing device (DE) for which it asks from physiological characterization which had information (FPAUTINF) used for a user's attestation detected.
- c) A means to input information (AUTINF) used for attestation via an input device (EE) which inputs information, and this input device.
- d) or [ having asked ] -- or test equipment (PE) which inspects inputted certification information, and releases a function of apparatus to a user of this \*\* when an inspection is effective.

**[Claim 2]**The apparatus according to claim 1 which as for said data processing device (DE) is constituted so that identically to certification information (FPPIN) asked for certification information (PIN) inputted via an input device for an inspection of effective attestation from physiological characterization of a user who has authority.

**[Claim 3]**The apparatus according to claim 1 or 2 by which said data processing device (DE) can use two or more processes (M1, ..., Mn) of searching for information (FPAUTINF1, ..., FPAUTINFn) used for attestation of a user of this \*\* from a user's detected physiological characterization.

**[Claim 4]**The apparatus according to claim 3 as which said data processing device makes a desired process choose from physiological characterization among two or more processes of searching for certification information, to a user who has authority.

**[Claim 5]**Apparatus given [ to claims 1-4 ] in any 1 paragraph which has a means to display certification information (FPAUTINF) searched for from a user's physiological characterization.

**[Claim 6]**A user has a means which attests by inputting certification information via an information input device, using physiological characterization peculiar to a user, In the 1st case, a sensor apparatus detects a user's physiological characterization, How to attest an equipment user characterized by what it inspects with test equipment in quest of information used for attestation from detected physiological characterization, and certification information which a user inputted via an input device in the 2nd case is inspected for with the same test equipment.

**[Claim 7]**A method of attesting the equipment user according to claim 6, comprising:

- a) A step which asks for a feature vector from measurement data of a sensor apparatus.
- b) A step which quantizes a vector from a called-for feature vector.
- c) A step which inspects certification information corresponding to a result of quantization of a vector.

---

[Translation done.]

\* NOTICES \*

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
3. In the drawings, any words are not translated.

---

## DETAILED DESCRIPTION

---

### [Detailed Description of the Invention]

#### [0001]

Before using, very various electronic equipment by which a user has to perform attestation thru/or authentication is known. The main example is, the computer (information management system) of various composition, communication equipment, for example, a mobile phone etc., etc. There are some which are generally protected by the password as opposed to the unauthorized use in these apparatus. Other apparatus has protected only the predetermined function against unlawful access (for example, what is called personal identification number PIN). Predetermined data or protection of access to service also belongs to this. That is right, even when this is not used by apparatus and used by a computer network or the communication network.

#### [0002]

The input of the certification information of the form used frequently today is an input through the keyboard of apparatus. The justification of information inputted after the input and by extension, the authority of the user who performed the input are inspected with the test equipment of apparatus, a computer network, or a communication network. In the mobile phone based on a GSM standard, this is performed by inspecting whether inputted PIN suits the information memorized by the SIM card using the data processing device on what is called a SIM card of apparatus. In suiting, a mobile phone becomes usable with a SIM card. Where PIN was not memorized and is locked in apparatus based on a GSM standard, when the SIM card memorizes, the security of the customer of a telephone goes up.

#### [0003]

The art which can attest a user in the form of others from before for a while is used. This art is based on detecting physiological characterization peculiar to a user by a special sensor. This main example is a fingerprint detection sensor. Another physiological characterization is the characteristic of the retina tissue the human being's eyes', or human being's voice, and these are similarly used by several sorts of apparatus.

#### [0004]

Usually, when the feature detected by the sensor is compared with the known feature of the user who has authority and is fully in agreement with apparatus or the data processing device of a communication network, access to the function of desired service, required data, or selected apparatus is released.

#### [0005]

It is significant if attestation of the two above-mentioned forms combines mutually in the apparatus of some types. For example, it is more desirable for a user not only to be able to use a telephone

with a fingerprint sensor, but to be able to share PIN with other persons, or to be able to use in a mobile phone, so that it can use within the limits of the authority to which apparatus is given with the peculiar SIM card. The attestation which furthermore passed the fingerprint generates an error accidentally, or becomes impracticable. This is a case where the user's hand is dirty or the user has stuck the glove. It is that desirable one (or required thing) can be attested from these reasons or other reasons by the technique by which one person differs from two or more users of apparatus. Physiological attestation is performed along with attestation by an PIN input in this case. In the mobile phone based on a GSM standard, this standard has defined the authentication means by an PIN input beforehand compulsorily.

[0006]

The above-mentioned situation shows that the conventional physiological authentication process is impossible in the mobile phone based on a GSM standard. It is because attestation by PIN using a SIM card is certainly required from the reason of compatibility over a GSM standard. As a means which looks possible for the time being, PIN is memorized in apparatus, and this is eliminated although it is possible to transfer PIN memorized in accordance with the detected fingerprint and the fingerprint with which the user who has authority was remembered when an inspection is effective to a SIM card, and to inspect it. It is because memorizing PIN at somewhere else other than the inside of a SIM card in a mobile phone is forbidden by the GSM standard from the reasons of security. Physiological attestation is taken into consideration as an additional security means in this case. However, such an additional security means is unnecessary if it carries out from the high safety of attestation by an PIN input, and many users cannot accept it easily and should sense it.

[0007]

The technical problem made into the foundation of this invention is providing the technical idea which makes possible combination of a physiological user's attestation, and attestation by an PIN input also in the mobile phone of a GSM standard or a similar case, and enables it to fully utilize attestation of each form. It has the option whether a user wants to use attestation of which form. However, it can have a means by which the especially selected user (for example, owner of apparatus) can adjust logic AND combination of two attestation forms in apparatus. This technical problem is solved by the claim by the apparatus or the method of a statement.

[0008]

In this invention, a user's physiological characterization is detected by a sensor apparatus, and the information used for attestation is searched for using a mathematical process from the detected physiological characterization. Certification information arises in the culmination which evaluates physiological characterization by this, and this information is inspected with the same test equipment as inspecting the certification information which the user inputted via the information input device (for example, keyboard). In the easiest case, the result of evaluation of a fingerprint becomes the same thing as PIN which the user inputted via the keyboard. However, this PIN is calculated from a user's physiological characterization detected by the sensor apparatus rather than is memorized by apparatus.

[0009]

It is not necessary to become equivalent [ attestation of this form ] to the result of attestation through the input of the keyboard according to the form of evaluating the physiological characterization detected by the sensor apparatus, and becomes unnecessary to change the usual interface which inspects the validity of attestation. It is not necessary to change a certain protocol standardized especially. The two techniques of attestation can be satisfactorily used in parallel. The user can choose two techniques freely in any state at any time. It can also constitute so that the two attestation techniques may give permission only to the user who passed effectively, of course using AND combination.

[0010]

This invention is explained in detail using figures according to an advantageous example below.

[0011]

The example of this invention by which all the methods and devices are accumulated into apparatus is shown in drawing 1.

[0012]

The example of this invention to which test equipment exists in apparatus is shown in drawing 2.

[0013]

The example of this invention on which the display which displays certification information is accumulated by apparatus is shown in drawing 3.

[0014]

An example typical and important for this invention moreover is a mobile phone based on a GSM standard, and this uses a fingerprint sensor for a user's attestation. This fingerprint sensor is a special example of sensor apparatus SE shown in drawing 1. If the user of the apparatus EG is standing by putting a finger on this fingerprint sensor and attesting the input of apparatus of PIN, SuperPIN, PIN2 (it is selectively dependent on a maker), etc., A fingerprint sensor detects suitable physiological characterization BM of the user of this \*\*, and sends this out to data processing device DE.

[0015]

In the case of a GSM mobile phone, this data processing device is with the processor already provided in the mobile phone, and the software which operates on this processor. However, on the other hand, the special software with which it is used via a peculiar processor unit (or generally sensor apparatus), and a fingerprint sensor manages fingerprint recognition on this processor unit operates. Thereby, the data processing device is incorporated in the sensor apparatus completely selectively in the range of this invention. Like other techniques of recognizing physiological characterization, since it is fully common knowledge at this work engineer, the real original form voice (and integration of partitioning in a subsystem, or a well-known hardware module), i.e., various configurations, of a data processing device, the fingerprint recognition itself, About this portion, there is no problem in particular in realization of the security of this invention.

[0016]

According to this invention, a data processing device searches for the information which was suitable for the user's attestation from the detected physiological characterization. It is PIN (or PIN2 in addition to this) memorized in the state where it was locked on the SIM card of the user regarded as this having authority in the easiest case. This PIN is handed over and inspected to a SIM card, as the user inputted via the keyboard (information input device) of a mobile phone. Next, to this work engineer, the inspection process provided in the well-known GSM standard operates within the test equipment (a SIM card, a device connected with the data processing device of apparatus by the case) of a mobile phone. When the certification information FPAUTINF is in agreement with PIN memorized on the right case, i.e., a SIM card, the functions (for example, network access etc.) of the apparatus protected by attestation are released.

[0017]

The important advantage of the means of above-mentioned this invention is that a fingerprint recognition part hands over a user's PIN to a SIM card, when the user has authority. It is because it is not necessary to change the security protocol of a GSM standard at all by this. This advantageous characteristic does not exist in a means by which it seems that others are fundamental. use any -- by the means of \*\*, the input of additional PIN through a keyboard is needed, or evasion thru/or change of a GSM standard is needed. The input through a keyboard of additional PIN is effective only when taking fingerprint recognition into consideration as an additional security means added to the PIN input.

[0018]

Of course, such additional attestation is possible also by this invention. In this case, it is not necessary to transmit the certification information searched for from sensor data to a SIM card.

Instead, for example, intentionally mistaken PIN may be transmitted to a SIM card, or an input error, discontinuation, others of an input, etc. may simulate. On the other hand, a SIM card newly requires an PIN input. In accordance with PIN asked for inputted PIN, when interexchangeable, data processing device DE transmits this PIN to a SIM card, and release is permitted according to this.

[0019]

PIN calculated from sensor data, of course may not necessarily be the same as that of PIN of a SIM card. By an above-mentioned standard or other apparatus, when a suitable security protocol grants a permission each time, test equipment can inspect whether these suit mutually by two different certification information.

[0020]

When there is the certification information FPAUTINF calculated from sensor data in other apparatus which is not based on a GSM standard only by one attestation (namely, attestation simultaneous with an PIN input or attestation independent of this) by sensor data, Although it may differ from the certification information AUTINF inputted via the keyboard, if two information directs the user who has authority, these will recognize test equipment to conform simultaneously.

[0021]

All the mathematical simulations (function) are fundamentally taken into consideration as a computation process over the certification information FPAUTINF acquired from physiological characterization BM. The certification information (generally coded by the alphanumeric character) AUTINF of other forms is assigned to a fingerprint or other physiological characterization BM. The following conditions must be satisfied here. namely, a -- the same certification information FPAUTINF being drawn from physiological characterization BM similar enough, and, b) The certification information FPAUTINF which is different from fully different physiological characterization BM is drawn, and what the certification information FPAUTINF is searched for from physiological characterization BM or the knowledge of this feature BM (for example, it guesses) is an impossible thing substantially for the user of c injustice.

[0022]

It guarantees that the conditions a fully have fingerprint recognition with a LOVA strike also to a small noise. Otherwise, it is because the rate that the user who has authority is refused will become very high. The conditions b are established so that a different user's fingerprint may derive the various certification information FPAUTINF with probability high enough to this. The meaning of the conditions c is clear.

[0023]

Various mathematical simulations which are satisfied with a person skilled in the art (there is some of appropriateness by a case) of this demand are common knowledge. The simulation which has these characteristics is given by what is called vector quantization. The technique of the common knowledge to a person skilled in the art is not explained other than the part considered to be here required for an understanding of this invention.

[0024]

It is premised on the physiological characterization detected by the sensor apparatus being first moved to the so-called form of a feature vector when using this technique for the purpose of this invention. This assumption does not turn into any limitation actually, either. It is because sensor data is expressed as n groups who were always able to set in order n measurement data (feature vector). A feature vector forms the space of n dimension. In this space, a set (code book vectors) of a pattern vector exists, and an interval scale (similar degree to physiological characterization) is specified. The cell in space exists to each pattern vector, this cell \*\*\*\*s in each feature vector in a cell, and the pattern vector is prescribed by being a cell of the pattern vector which exists in the next within the limits of the interval scale of this \*\*.

[0025]

The information for which it was fundamentally suitable in attestation is assigned to each pattern

vector. Exact certification information (for example, true PIN) is assigned to one pattern vector. If it asks for the pattern vector which exists in the next to the predetermined feature vector which \*\*\*\*s to the detected sensor data so that clearly from the above-mentioned explanation, when the user of this \*\* has authority, exact information (true PIN) is drawn, and when that is not right, the mistaken certification information will be sent out. The error rate of this process can be optimized when it is guaranteed that the feature vector relevant to the physiological characterization of the user who has authority is one of the pattern vectors. This is attained by adapting this system to the physiological characterization of the user who has authority in an initialization phase (code book adaptation).

[0026]

Vector quantization is not the only technique which can be used in relation to this invention. Other techniques which are not explained to a person skilled in the art here are feasible.

[0027]

Originally calculating the certification information FPAUTINF by vector quantization from a user's physiological characterization is connected with "memory of PIN" by apparatus (if based on this specification). It is because the possible certification information FPAUTINF is fundamentally assigned to each pattern vector of a code book. However, this is actually (except for one user's, i.e., the user who has authority, feature vector) suitable for attestation in almost no cases. That is, for example, although all the possible PIN is memorized ideally and a pattern vector is assigned to every one each of these in PIN of the alphanumeric character of 5 figures, only when a pattern vector is detected correctly enough, addressing can be carried out to appropriate PIN within a sensor. It will become impossible therefore, to find out exact PIN in spite of "memorizing in apparatus" except the user who has the exact physiological characterization in which the number of possible PIN becomes large too much. Such a situation is not taken into consideration when memorizing PIN to apparatus by a standard is forbidden.

[0028]

Memorizing PIN to apparatus is not permitted in a GSM standard. However, the necessity of changing PIN is produced frequently. This is a case where PIN is known by the 3rd person etc. However, it is that which calculates PIN from a fingerprint in this invention (that is, it calculates), and unless exchange of a fingerprint or other physiological characterizations is possible, this is impossible first. If a means to change PIN is still given to a user, it constitutes so that it may replace only with one computation process and all the sets of this kind in apparatus of process can be equally used by the advantageous embodiment of this invention. The sequence number is assigned to each computation process and the user who has authority to this can change the process to be used at any time. Since each process M1 and ... to the same fingerprint BM, and Mn calculate other PIN (FPAUTINF1, ..., FPAUTINFn), it is chosen whether a user makes much PIN calculate in which process.

[0029]

The example of this invention is realizable by vector quantization similarly. Not only a code book but two or more code books of the pattern vector are provided here. Each code book has a predetermined number and it is selectable via this number in it. Probably it depends for other processes on a parameter. In this invention, other mathematical simulations are formed by changing this parameter. If the dependency of a parameter is complicated enough, even if it changes a parameter actually, the guess of change of certification information will become impossible. The neural network (what is called multilayer perceptron) of a predetermined type is suitable for realizing this kind of simulation. By the means based on this neural network, actually, anywhere, PIN is not memorized as a sign sequence but is only memorized by network architecture as a weighting coefficient (in the state where it was locked suggestively).

[0030]

Especially in this example of this invention, it is taken into consideration from a viewpoint for which

the sequence of the password with which many persons differ is needed to the thoroughly different purpose or apparatus. It should become increasingly difficult to care about many passwords. When two or more processes  $M_1, \dots, M_n$  (mathematical simulation) are used for the calculation from the only feature vector (sensor data aggregate) of two or more certification information (FPAUTINF1, FPAUTINF2), The problem at the time of detecting the physiological characterization which is not made to \*\*\*\* peculiar to a user is reduced by a suitable sensor.

[0031]

What is necessary is just to input the index of this kind of process in the context only provided in the user's operation table side, in order to choose a predetermined process. Thereby, a data processing device can constitute suitably for every software.

[0032]

Of course, two or more persons' physiological characterization is also combinable with one or more right PIN. When apparatus is combined only with one person as an exception (i.e., when only one SIM card is used correctly), release can be additionally combined with other security mechanisms, for example, the code of apparatus, etc. According to this invention, the pliability of each form, high safety, and the compatibility over a standard are acquired here.

[0033]

When changing PIN, the display for presenting of certification information is formed in another, especially advantageous example of this invention. Since this kind of displays are this kind of apparatus [ much ] and have already existed since the start, this can be used for this purpose. If it is going to change the certification information AUTINF (for example, PIN) which the user inputted via the keyboard into the information which suits a SIM card, in some computation processes, combination of the number of all the possible signs cannot use it as PIN by a case. For example, it is because it is smaller than the number of all the PIN in which a code book is possible. This case is enough to assign PIN to a pattern vector and change PIN corresponding to an individual pattern vector if the parameter of the computation process used is changed (for example, change of a code book number or change of a neural network's parameter). If PIN (or PIN which should generally be inputted) on a SIM card is not known after that, it becomes impossible to change in this meaning. And this is required because of the further use to the technical problem of this invention. The user who has authority can be told about changed PIN by making the display of apparatus give a short-time indication only once suitably, advantageously, after changing PIN. Other means (for example, show new PIN later) are possible.

[0034]

Of course, this invention is not limited to a mobile phone, for example, the mobile phone based on a GSM standard. It is not difficult for a person skilled in the art to realize this invention in other apparatus or other systems based on the above-mentioned explanation, either.

[0035]

This invention in particular is not limited only to the case where inspection unit PE is accumulated into apparatus. The important example of apparatus is shown in drawing 2, apparatus is connected with other at least one apparatus via a communication network, and test equipment also exists in a network here. The portion which manages calculating the certification information FPAUTINF from a part of data processing device or data processing unit DE, i.e., a user's physiological characterization BM, does not necessarily need to exist in apparatus, either. Of course, apparatus does not need to have accumulated sensor apparatus SE or accumulated keyboard EE. It is also clear that a device may be connected to apparatus in the form of an external module. The example of this invention should be protected by the claim of the method.

[Brief Description of the Drawings]

[Drawing 1]

All the methods and devices are the figures showing the example of this invention accumulated into apparatus.

**[Drawing 2]**

All the methods and devices are the figures showing the example of this invention accumulated into apparatus.

**[Drawing 3]**

The display which displays certification information is a figure showing the example of this invention accumulated by apparatus.

---

[Translation done.]

**\* NOTICES \***

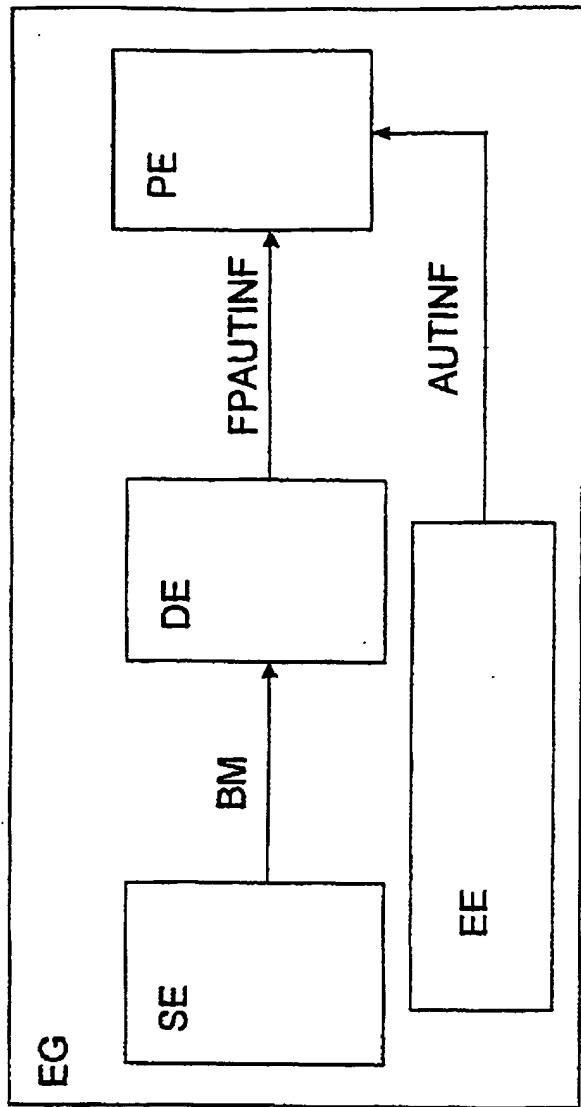
JPO and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
3. In the drawings, any words are not translated.

---

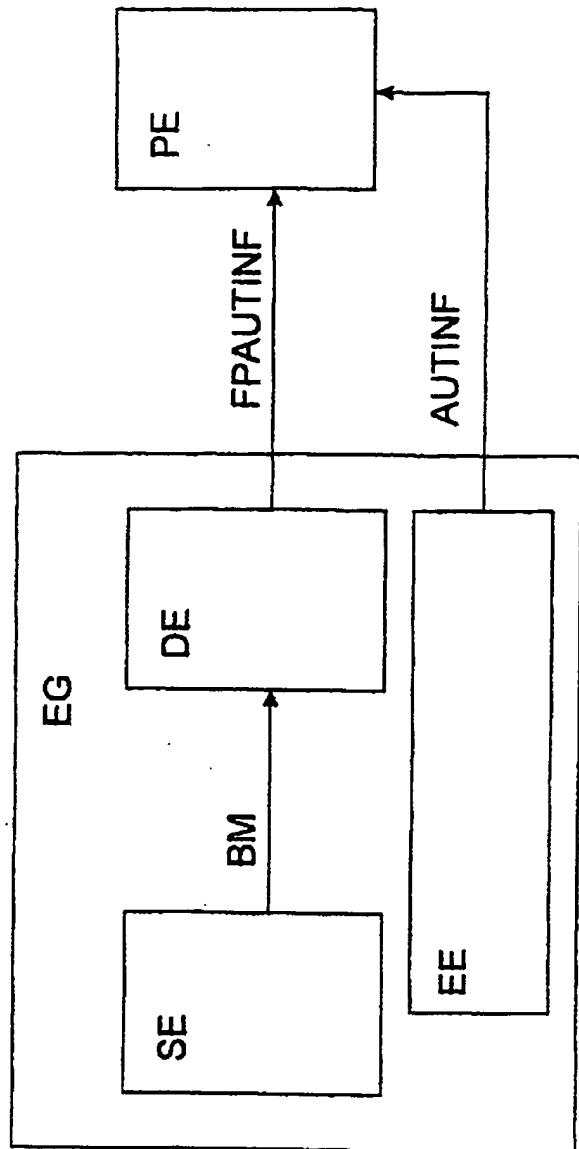
**DRAWINGS****[Drawing 1]**

FIG 1



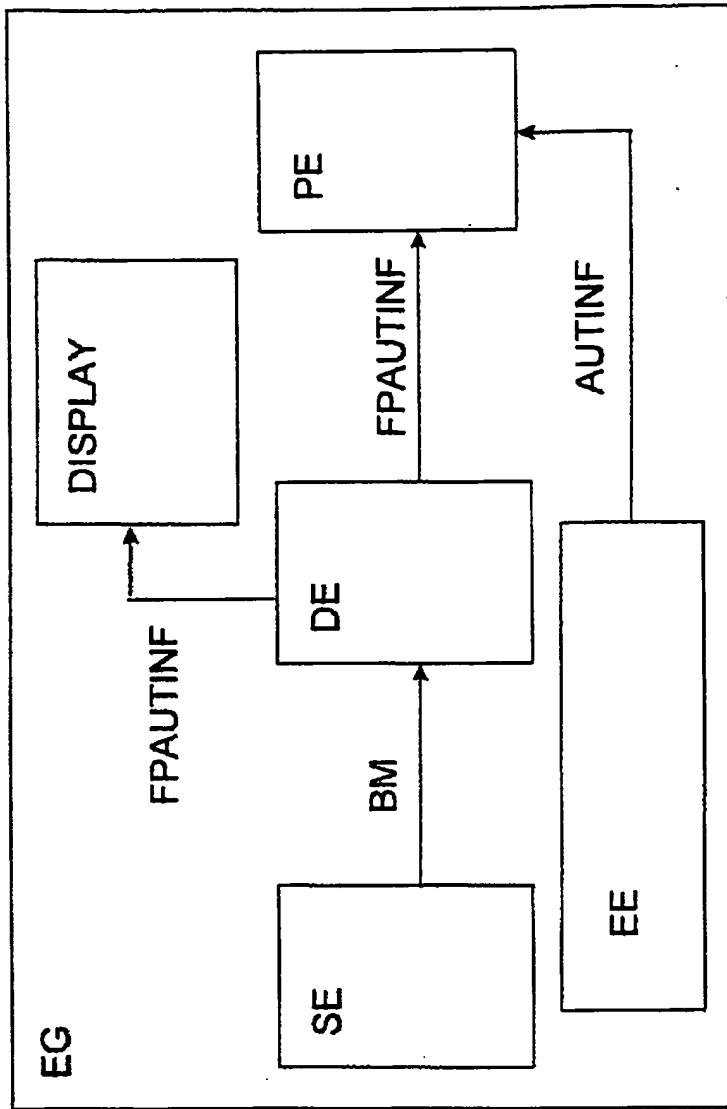
[Drawing 2]

FIG 2



[Drawing 3]

FIG 3



---

[Translation done.]